



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,421	03/26/2004	Fusao Ishiguchi	04536.034001	2620
22511 7590 10/30/2008 OSHA LIANG I.L.P. TWO HOUSTON CENTER 909 FANNIN, SUITE 3500 HOUSTON, TX 77010				
EXAMINER				
HAILU, TESHOME				
ART UNIT		PAPER NUMBER		
2439				
NOTIFICATION DATE		DELIVERY MODE		
10/30/2008		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
buta@oshaliang.com

Office Action Summary

Application No.

10/811,421

Applicant(s)

ISHIGUCHI, FUSAO

Examiner

TESHOME HAILU

Art Unit

2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 August 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SF/ICE)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 25, 2008 has been entered.
2. Claims 1-8 have been amended.
3. Claims 1-8 are pending.

Response to Amendment

4. Applicant's arguments filed August 25, 2008, with respect to 35 USC 112 rejections of claims 1, 5 and 8 have been fully considered in view of the amendment and are persuasive. The 35 USC 112 rejections of claims 1, 5 and 8 have been withdrawn.
5. Applicant's arguments filed on August 25, 2008, with respect to 35 USC 103(a) rejections of claims 1-8 have been fully considered but they are not persuasive.
6. Applicant argues that Doiron (US 5,481,610) fails to teach the limitation, "a flash memory in which key data is written at a prescribed address in an unused area of the flash memory" as recited in claims 1, 5 and 8. Also applicant mentioned that Doiron fails to disclose "the key data is protected from third parties because the prescribed address is unknown". Examiner disagrees.
7. Examiner would point out that, Doiron teaches this limitation as (column , line , the starting address of the encrypted key block 86 is variable according to a starting address calculated as a function of values 82, 84 (the variability occurs because value 82 is also pseudo-random number albeit limited in range). In accordance with an important aspect of the present invention, every time the key loader 100 is

attached, a new pseudo-random data value 82 is written to table 78 thus changing the starting location of the encrypted key block 86). According to Doiron, each time the new key is loaded to the memory location (fig. 3, block 86) the starting location the key block is changed and it will be impossible for the parties to know the location of the stored key.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doiron et al (US 5,481,610) in view of Nakano (US Pub. No. 2003/0182565).

As per claim 1 Doiron discloses:

A digital video disc device, comprising: a flash memory in which key data associated with information on a digital video disc is recorded in advance in a prescribed address in an unused specific area; (abstract, line 1-6, a digital radio has standardized "key" storage for several different cryptosystems (DES, VGE, VGS, etc.). Cryptographic keys are stored in a table in non-volatile memory such as EEPROM). Also see fig. 2.

Wherein random data is written in all of the unused area around an area where said key data is recorded in said specific area of said flash memory, (column 4, line 18-37, a digital radio has standardized "key" storage for several different cryptosystems (DES, VGE, VGS, etc.). Cryptographic keys are stored in a table in non-volatile memory such as EEPROM. As a result, the stored key itself

looks like the stored random data and it would be hard for an attacker to identify the cryptographic keys from the random data). Also see the table in fig.3

Means for accessing the information on said digital video disc using said key data read from said prescribed address in said flash memory; (column 1, line 5-13, the invention relates to radio frequency (RF) communications systems, and more particularly to digital radios having a "secure" mode that encrypts and decrypts messages. Still more particularly, the present invention relates to techniques for securely loading and storing cryptographic key information within a mobile or portable radio transceiver).

Doiron does not explicitly disclose, the information on a digital video disk. However, in the same field of endeavor, Nakano teaches this limitation as, (page , paragraph 7, the DVD right protection system each DVD reproduction terminal for reproducing digital content recorded on a distributed DVD pre-stores a master key. The master key is determined by the manufacturer of the particular reproduction terminal. The reproduction terminal, which uses this master key in the decryption process, has a function of ultimately decrypting and reproducing the digital content recorded on the DVD).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Doiron and include the information on a digital video disk using the teaching of Nakano in order to substitute one method for the other to achieve the predictable result of securing information in electronic media using the key data stored in memory.

The key data is configured to be modified by a key data writing equipment. (Column 10, line 60-65, as cryptographic keys are loaded into the bank 86, the bit-mask byte 90 is updated to indicate which keys within the bank are valid).

Doiron does not explicitly disclose that the key data can be modified by key data writing equipment. However, in the same field of endeavor, Nakano teaches this limitation as, (page, paragraph 113, the key setting system 104 has a key information storage unit 301, a key information generation unit 302, an invalid terminal designation unit 303, a key information updating unit 304, a decryption key determining unit 305, and an encryption key designation unit 306). Both the key information generation unit (writing equipment) and key information updating unit (modifying) are a part of key setting system (see fig. 3 of Nakano).

Therefore, it would have been obvious to one of ordinary skill in the art, at the time of the invention was made, to modify the teaching of Doiron and include the limitation, "the key data can be modified by key data writing equipment", using the teaching of Nakano in order to make the key information valid by updating (modifying) with right and most up-to-date information (see paragraph 117 of Nakano).

Claims 5 and 8 are rejected under the same reason set forth in rejection of claim 1:

As per claim 2 Doiron in view of Nakano discloses:

The equipment for a digital video disc according to claim 1, wherein said key data is an encryption key for equipment for encrypting and recording the information on said digital video disc. (Column 8, line 1-33, the EEPROM 76 that stores a key table 78 containing cryptographic keys to be used for encrypting and decrypting purpose by encryptor/decryptor 74).

As per claims 3 in view of Nakano discloses:

The equipment for a digital video disc according to claim 2, wherein said key data is a decryption key for equipment for decrypting the information read from said digital video disc. (Column 8, line 1-33, the EEPROM 76 that stores a key table 78 containing cryptographic keys to be used for encrypting and decrypting purpose by encryptor/decryptor 74).

Claim 4 is rejected under the same reason set forth in rejection of claim 3:

As per claim 6 Doiron in view of Nakano discloses:

The method of recording prescribed information according to claim 5, wherein said memory is mounted on equipment for a digital video disc, (see the EEPROM on fig. 2).

Said prescribed information is key data associated with information on a digital video disc. (Column 9, line 33-52, "meaningful" data stored within table 78 includes a first byte random value 82, a

kth byte random value 84, and at least one (and typically many) cryptographic keys stored in key banks residing within a cryptographic key block 86).

As per claim 7 Doiron in view of Nakano discloses:

The method of recording prescribed information according to claim 5, wherein said prescribed information is a password. (Column 8, line 1-33, the EEPROM 76 that stores a key table 78 containing cryptographic keys to be used for encrypting and decrypting purpose by encryptor/decryptor 74).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TESHOME HAILU whose telephone number is (571)270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Teshome Hailu

October 25, 2008
/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434